

netwerkbeveiligingsbeleid: witboek over beste praktijken

Inhoud

[Inleiding](#)
[voorbereiding](#)
[Gebruiksbeleidsverklaringen maken](#)
[Voer een risicoanalyse uit](#)
[Opzetten van een Security Team Structuur](#)
[preventie](#)
[Beveiligingswijzigingen goedkeuren](#)
[Beveiliging van uw netwerk](#)
[antwoord](#)
[Beveiligingsovertredingen](#)
[restauratie](#)
[recensie](#)
[Gerelateerde informatie](#)

Inleiding

Zonder beveiligingsbeleid kan de beschikbaarheid van uw netwerk in gevaar komen. Het beleid begint met het beoordelen van het risico voor het netwerk en het opbouwen van een team om te reageren. Voortzetting van het beleid vereist het implementeren van een security change management praktijk en het monitoren van het netwerk voor inbreuken op de beveiliging. Tot slot wijzigt het evaluatieproces het bestaande beleid en past het zich aan de geleerde lessen aan.

Dit document is verdeeld in drie gebieden: [voorbereiding](#), [preventie](#) en [reactie](#). Laten we elk van deze stappen in detail bekijken.

voorbereiding

Voordat u een beveiligingsbeleid implementeert, moet u het volgende doen:

- [Gebruiksbeleidsverklaringen maken](#).
- [Voer een risicoanalyse uit](#).
- [Creëer een security team structuur](#).

Gebruiksbeleidsverklaringen maken

We raden aan gebruiksbeleidsverklaringen te maken waarin de rollen en verantwoordelijkheden

van gebruikers met betrekking tot beveiliging worden beschreven. U kunt beginnen met een algemeen beleid dat betrekking heeft op alle netwerksystemen en gegevens binnen uw bedrijf. Dit document moet de algemene gebruikersgemeenschap inzicht geven in het beveiligingsbeleid, het doel ervan, richtlijnen voor het verbeteren van hun beveiligingspraktijken en definities van hun beveiligingsverantwoordelijkheden. Als uw bedrijf specifieke acties heeft geïdentificeerd die kunnen leiden tot strafmaatregelen of disciplinaire maatregelen tegen een werknemer, moeten deze acties en hoe ze te vermijden duidelijk in dit document worden verwoord.

De volgende stap is het opstellen van een acceptabele gebruiksverklaring voor partners om partners inzicht te geven in de informatie die voor hen beschikbaar is, de verwachte beschikbaarheid van die informatie en het gedrag van de werknemers van uw bedrijf. U moet duidelijk uitleggen welke specifieke handelingen zijn geïdentificeerd als beveiligingsaanvallen en welke strafmaatregelen zullen worden genomen als een beveiligingsaanval wordt gedetecteerd.

Maak ten slotte een verklaring voor acceptabel gebruik door de beheerder om de procedures voor het beheer van gebruikersaccounts, beleidshandhaving en privilegecontrole uit te leggen. Als uw bedrijf specifieke beleidsregels heeft met betrekking tot gebruikerswachtwoorden of de daaropvolgende verwerking van gegevens, moet u die beleidsregels ook duidelijk presenteren. Controleer het beleid tegen de partner acceptabel gebruik en de gebruiker acceptabel gebruik beleidsverklaringen om uniformiteit te garanderen. Zorg ervoor dat de beheerdersvereisten die in het beleid voor acceptabel gebruik worden vermeld, worden weerspiegeld in trainingsplannen en prestatiebeoordelingen.

Voer een risicoanalyse uit

Een risicoanalyse moet de risico's voor uw netwerk, netwerkbronnen en gegevens identificeren. Dit betekent niet dat u elk mogelijk toegangspunt tot het netwerk moet identificeren, noch elk mogelijk aanvalsmiddel. De bedoeling van een risicoanalyse is om delen van uw netwerk te identificeren, een dreigingsbeoordeling aan elk deel toe te wijzen en een passend beveiligingsniveau toe te passen. Dit zorgt voor een werkbare balans tussen beveiliging en vereiste netwerktoegang.

Wijs elke netwerkbron een van de volgende drie risiconiveaus toe:

- Systemen met een laag risico of gegevens die bij compromittering (gegevens die door onbevoegd personeel worden bekeken, gegevens die beschadigd zijn of gegevens die verloren gaan) het bedrijf niet zouden verstoren of juridische of financiële gevolgen zouden hebben. Het doelsysteem of de gegevens kunnen eenvoudig worden hersteld en bieden geen verdere toegang tot andere systemen.
- Systemen met een gemiddeld risico of gegevens die bij compromittering (gegevens die door onbevoegd personeel worden bekeken, gegevens die beschadigd zijn of gegevens die verloren gaan) een matige verstoring van het bedrijf, kleine juridische of financiële gevolgen zouden veroorzaken of verdere toegang tot andere systemen zouden bieden. Het doelsysteem of de gegevens vereisen een matige inspanning om het systeem te herstellen of het herstelproces is storend voor het systeem.
- Hoog risico systemen of gegevens die, indien gecompromitteerd (gegevens bekeken door

onbevoegd personeel, gegevens beschadigd, of gegevens verloren) een extreme verstoring in het bedrijf zou veroorzaken, grote juridische of financiële gevolgen zou veroorzaken, of bedreigen de gezondheid en veiligheid van een persoon. Het beoogde systeem of de beoogde gegevens vergen aanzienlijke inspanningen om te herstellen of het herstelproces is storend voor het bedrijf of andere systemen.

Wijst een risiconiveau toe aan elk van de volgende kernnetwerkapparaten, distributienetwerkapparaten, toegangsnetwerkapparaten, netwerkbewakingsapparaten (SNMP-monitoren en RMON-sondes), netwerkbeveiligingsapparaten (RADIUS en TACACS), e-mailsystemen, netwerkbestandsservers, netwerkafdrukservers, netwerktoepassingsservers (DNS en DHCP), gegevenstoepassingsservers (Oracle of andere zelfstandige toepassingen), desktopcomputers en andere apparaten (zelfstandige afdrukservers en netwerfaxmachines).

Netwerkapparatuur zoals switches, routers, DNS-servers en DHCP-servers kunnen verdere toegang tot het netwerk mogelijk maken en zijn daarom apparaten met een gemiddeld of hoog risico. Het is ook mogelijk dat corruptie van deze apparatuur het netwerk zelf kan doen instorten. Een dergelijke mislukking kan zeer versturend zijn voor het bedrijf.

Zodra u een risiconiveau hebt toegewezen, is het noodzakelijk om de soorten gebruikers van dat systeem te identificeren. De vijf meest voorkomende soorten gebruikers zijn:

- Beheerders Interne gebruikers die verantwoordelijk zijn voor netwerkbronnen.
- Bevoorrechte interne gebruikers met behoefte aan meer toegang.
- Gebruikers met algemene toegang.
- Partners Externe gebruikers met een behoefte om toegang te krijgen tot sommige bronnen.
- Andere externe gebruikers of klanten.

De identificatie van het risiconiveau en het type toegang dat voor elk netwerksysteem vereist is, vormt de basis van de volgende beveiligingsmatrix. De beveiligingsmatrix biedt een snelle referentie voor elk systeem en een startpunt voor verdere beveiligingsmaatregelen, zoals het creëren van een geschikte strategie voor het beperken van de toegang tot netwerkbronnen.

systeem	Beschrijving	risiconiveau	Soorten gebruikers
ATM-switches	Kernnetwerkapparaat	Hoog	Beheerders voor apparaatconfiguratie (alleen ondersteuningspersoneel); Alle andere voor gebruik als transport
Netwerkrouters	Distributienetwerkapparaat	Hoog	Beheerders voor apparaatconfiguratie (alleen ondersteuningspersoneel); Alle andere voor gebruik

			als transport
Kast switches	Toegangsnetwerkkapparaat	Gemiddeld	Beheerders voor apparaatconfiguratie (alleen ondersteuningspersoneel); Alle andere voor gebruik als transport
ISDN- of inbelservers	Toegangsnetwerkkapparaat	Gemiddeld	Beheerders voor apparaatconfiguratie (alleen ondersteuningspersoneel); Partners en bevoorrechte gebruikers voor speciale toegang
firewall	Toegangsnetwerkkapparaat	Hoog	Beheerders voor apparaatconfiguratie (alleen ondersteuningspersoneel); Alle andere voor gebruik als transport
DNS- en DHCP-servers	Netwerktoeepassingen	Gemiddeld	Beheerders voor configuratie; Algemene en bevoorrechte gebruikers voor gebruik
Externe e-mailserver	Netwerktoeepassing	Laag	Beheerders voor configuratie; Alle andere voor postvervoer tussen het internet en de interne mailserver
Interne e-mailserver	Netwerktoeepassing	Gemiddeld	Beheerders voor configuratie; Alle andere interne gebruikers voor gebruik
Oracle-database	Netwerktoeepassing	Middelhoog of hoog	Beheerders voor systeembeheer; Bevoorrechte gebruikers voor gegevensupdates; Algemene gebruikers voor gegevenstoegang; Alle andere voor gedeeltelijke gegevenstoegang

Opzetten van een Security Team Structuur

Creëer een cross-functioneel beveiligingsteam onder leiding van een Security Manager met deelnemers uit elk van de operationele gebieden van uw bedrijf. De vertegenwoordigers in het team moeten op de hoogte zijn van het beveiligingsbeleid en de technische aspecten van het ontwerp en de implementatie van de beveiliging. Dit vraagt vaak om extra training voor de teamleden. Het beveiligingsteam heeft drie verantwoordelijkheden: beleidsontwikkeling, praktijk en reactie.

Beleidsontwikkeling is gericht op het opstellen en herzien van beveiligingsbeleid voor het bedrijf. Herzie ten minste de risicoanalyse en het veiligheidsbeleid op jaarbasis.

Praktijk is de fase waarin het beveiligingsteam de risicoanalyse uitvoert, de goedkeuring van verzoeken om wijzigingen in de beveiliging, beveiligingswaarschuwingen van zowel leveranciers als de [CERT](#) -mailinglijst beoordeelt en vereisten voor het beveiligingsbeleid in duidelijke taal omzet in specifieke technische implementaties.

Het laatste gebied van verantwoordelijkheid is respons. Hoewel netwerkbewaking vaak een beveiligingsovertreding identificeert, zijn het de leden van het beveiligingsteam die de werkelijke probleemoplossing en vaststelling van een dergelijke overtreding uitvoeren. Elk lid van het beveiligingsteam moet in detail op de hoogte zijn van de beveiligingsfuncties die door de apparatuur in zijn of haar operationele gebied worden geleverd.

Hoewel we de verantwoordelijkheden van het team als geheel hebben gedefinieerd, moet u de individuele rollen en verantwoordelijkheden van de leden van het beveiligingsteam in uw beveiligingsbeleid definiëren.

preventie

Preventie kan in twee delen worden opgesplitst: [het goedkeuren van beveiligingswijzigingen](#) en het [bewaken van de beveiliging van uw netwerk](#).

Beveiligingswijzigingen goedkeuren

Beveiligingswijzigingen worden gedefinieerd als wijzigingen in netwerkapparatuur die een mogelijke impact hebben op de algehele beveiliging van het netwerk. Uw beveiligingsbeleid moet specifieke vereisten voor beveiligingsconfiguratie in niet-technische termen identificeren. Met andere woorden, in plaats van een vereiste te definiëren als "Geen externe bronnen FTP-verbindingen zijn toegestaan via de firewall", definieert u de vereiste als "Externe verbindingen mogen geen bestanden van het interne netwerk kunnen ophalen". U moet een unieke reeks vereisten voor uw organisatie definiëren.

Het beveiligingsteam moet de lijst met vereisten voor onbewerkte talen bekijken om specifieke netwerkconfiguratie- of ontwerpproblemen te identificeren die aan de vereisten voldoen. Zodra het team de vereiste netwerkconfiguratie wijzigingen heeft gemaakt om het beveiligingsbeleid te implementeren, kunt u deze toepassen op toekomstige configuratiewijzigingen. Hoewel het mogelijk is voor het beveiligingsteam om alle wijzigingen te beoordelen, stelt dit proces hen in staat om alleen wijzigingen te beoordelen die voldoende risico vormen om een speciale behandeling te rechtvaardigen.

We raden het beveiligingsteam aan om de volgende soorten wijzigingen door te nemen:

- Elke wijziging in de firewallconfiguratie.
- Elke wijziging in toegangscontrolelijsten (ACL).
- Elke wijziging in de configuratie van het Simple Network Management Protocol (SNMP).
- Elke wijziging of update in software die afwijkt van de lijst met goedgekeurde revisieniveaus.

We raden ook aan de volgende richtlijnen te volgen:

- Wijzig wachtwoorden routinematig in netwerkapparaten.
- Beperk de toegang tot netwerkapparaten tot een goedgekeurde personeelslijst.
- Zorg ervoor dat de huidige softwarerevisieniveaus van netwerkapparatuur en serveromgevingen voldoen aan de vereisten voor beveiligingsconfiguratie.

Naast deze goedkeuringsrichtlijnen moet een vertegenwoordiger van het beveiligingsteam zitting nemen in de goedkeuringsraad van het wijzigingsmanagement om alle wijzigingen die het bestuur beoordeelt, te controleren. De vertegenwoordiger van het beveiligingsteam kan elke wijziging die als een beveiligingswijziging wordt beschouwd, weigeren totdat deze is goedgekeurd door het beveiligingsteam.

Beveiliging van uw netwerk

Beveiligingsbewaking is vergelijkbaar met netwerkbewaking, behalve dat het zich richt op het detecteren van wijzigingen in het netwerk die wijzen op een beveiligingsovertreding. Het uitgangspunt voor security monitoring is het bepalen van wat een overtreding is. In [een risicoanalyse](#) hebben we vastgesteld welk niveau van monitoring vereist is op basis van de bedreiging voor het systeem. Bij het [goedkeuren van beveiligingswijzigingen](#) hebben we specifieke bedreigingen voor het netwerk geïdentificeerd. Door naar beide parameters te kijken, ontwikkelen we een duidelijk beeld van wat u moet controleren en hoe vaak.

In de [risicoanalysematrix](#) wordt de firewall beschouwd als een risicovol netwerkapparaat, wat aangeeft dat u deze in realtime moet controleren. In het gedeelte [Beveiligingswijzigingen goedkeuren](#) ziet u dat u moet controleren op eventuele wijzigingen in de firewall. Dit betekent dat de SNMP-stembureau zaken als mislukte inlogpogingen, ongebruikelijk verkeer, wijzigingen in de firewall, toegang tot de firewall en verbindingen via de firewall moet controleren.

Maak in dit voorbeeld een monitoringbeleid voor elk gebied dat in uw risicoanalyse wordt geïdentificeerd. We raden aan om wekelijks apparatuur met een laag risico, apparatuur met een gemiddeld risico en apparatuur met een hoog risico te controleren. Als u snellere detectie nodig hebt, controleert u op een kortere tijdsperiode.

Ten slotte moet uw beveiligingsbeleid betrekking hebben op het melden van beveiligingsovertredingen aan het beveiligingsteam. Vaak is uw netwerkbewakingssoftware de eerste om de overtreding te detecteren. Het moet een melding naar het operatiecentrum

activeren, dat op zijn beurt het beveiligingsteam moet informeren, indien nodig met behulp van een semafoon.

antwoord

Het antwoord kan in drie delen worden opgesplitst: [beveiligingsovertredingen](#), [herstel](#) en [beoordeling](#).

Beveiligingsovertredingen

Wanneer een overtreding wordt gedetecteerd, is de mogelijkheid om netwerkapparatuur te beschermen, de omvang van de inbraak te bepalen en normale bewerkingen te herstellen afhankelijk van snelle beslissingen. Als u deze beslissingen van tevoren neemt, is het reageren op een inbraak veel hanteerbaarder.

De eerste actie na de detectie van een inbraak is de melding van het beveiligingsteam. Zonder een procedure zal er aanzienlijke vertraging zijn om de juiste mensen de juiste reactie te laten toepassen. Definieer een procedure in uw beveiligingsbeleid die 24 uur per dag, 7 dagen per week beschikbaar is.

Vervolgens moet u het niveau van de bevoegdheid die aan het beveiligingsteam om wijzigingen aan te brengen, en in welke volgorde de wijzigingen moeten worden gemaakt definiëren.

Mogelijke corrigerende maatregelen zijn:

- Wijzigingen doorvoeren om verdere toegang tot de overtreding te voorkomen.
- Isoleren van de geschonden systemen.
- Neem contact op met de provider of ISP in een poging de aanval te traceren.
- Gebruik van opnameapparatuur om bewijs te verzamelen.
- Verbinding verbreken met geschonden systemen of de bron van de overtreding.
- Contact opnemen met de politie of andere overheidsinstanties.
- Afsluiten van geschonden systemen.
- Systemen herstellen volgens een lijst met prioriteiten.
- Kennisgeving aan intern leidinggevend en juridisch personeel.

Zorg ervoor dat alle wijzigingen die kunnen worden uitgevoerd zonder goedkeuring van het management in het beveiligingsbeleid worden beschreven.

Tot slot zijn er twee redenen om informatie te verzamelen en bij te houden tijdens een beveiligingsaanval: om te bepalen in welke mate systemen zijn aangetast door een beveiligingsaanval en om externe schendingen te vervolgen. Het type informatie en de manier waarop u deze verzamelt, verschilt afhankelijk van uw doel.

Om de omvang van de overtreding te bepalen, doet u het volgende:

- Noteer de gebeurtenis door het verkrijgen van sniffer-sporen van het netwerk, kopieën van logbestanden, actieve gebruikersaccounts en netwerkverbindingen.
- Beperk verdere compromissen door accounts uit te schakelen, netwerkapparatuur los te koppelen van het netwerk en de verbinding met internet te verbreken.
- Maak een back-up van het gecompromitteerde systeem om te helpen bij een gedetailleerde analyse van de schade en de aanvalsmethode.
- Zoek naar andere tekenen van een compromis. Vaak wanneer een systeem wordt aangetast, zijn er andere systemen of accounts betrokken.
- Onderhoud en controleer logbestanden van beveiligingsapparaten en netwerkbewakingslogbestanden, omdat deze vaak aanwijzingen geven voor de aanvalsmethode.

Als u geïnteresseerd bent in het nemen van juridische stappen, laat uw juridische afdeling de procedures voor het verzamelen van bewijs en betrokkenheid van de autoriteiten bekijken. Een dergelijke toetsing verhoogt de doeltreffendheid van het bewijsmateriaal in gerechtelijke procedures. Als de overtreding intern van aard was, neem dan contact op met uw Human Resources-afdeling.

restauratie

Herstel van normale netwerkbewerkingen is het uiteindelijke doel van een reactie op een schending van de beveiliging. Definieer in het beveiligingsbeleid hoe u normale back-ups uitvoert, beveiligt en beschikbaar stelt. Aangezien elk systeem zijn eigen middelen en procedures heeft voor het maken van back-ups, moet het beveiligingsbeleid fungeren als een meta-beleid, waarin voor elk systeem de beveiligingsvoorwaarden worden beschreven die vanaf de back-up moeten worden hersteld. Als goedkeuring vereist is voordat restauratie kan worden uitgevoerd, moet u ook het proces voor het verkrijgen van goedkeuring opnemen.

recensie

Het herzieningsproces is de laatste stap in het creëren en onderhouden van een veiligheidsbeleid. Er zijn drie dingen die u moet beoordelen: beleid, houding en praktijk.

Het veiligheidsbeleid moet een levend document zijn dat zich aanpast aan een steeds veranderende omgeving. Door het bestaande beleid te toetsen aan bekende best practices blijft het netwerk up-to-date. Controleer ook de [CERT-website](#) voor nuttige tips, praktijken, beveiligingsverbeteringen en waarschuwingen die in uw beveiligingsbeleid kunnen worden opgenomen.

U moet ook de positie van het netwerk bekijken in vergelijking met de gewenste beveiligingspositie. Een extern bedrijf dat gespecialiseerd is in beveiliging kan proberen het netwerk binnen te dringen en niet alleen de positie van het netwerk te testen, maar ook de

beveiligingsreactie van uw organisatie. Voor netwerken met een hoge beschikbaarheid raden we aan jaarlijks een dergelijke test uit te voeren.

Ten slotte wordt de praktijk gedefinieerd als een oefening of test van het ondersteunend personeel om ervoor te zorgen dat ze een duidelijk begrip hebben van wat ze moeten doen tijdens een beveiligingsovertreding. Vaak wordt deze oefening onaangekondigd door het management en gedaan in combinatie met de netwerkpostuur test. In deze evaluatie worden lacunes in de procedures en de opleiding van personeel vastgesteld, zodat corrigerende maatregelen kunnen worden genomen.

Gerelateerde informatie

- [Meer white papers over beste praktijken](#)
- [Technische ondersteuning – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.